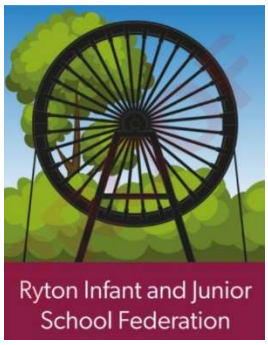
Ryton Infant and Junior School Federation

# E-Safety Policy

Last Reviewed: October 2020



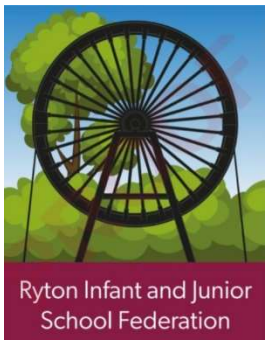

# Contents:

1. Teaching and learning
2. Managing internet access
3. Policy decisions
4. Pupil online safety curriculum
5. Communications policy

**Appendices**

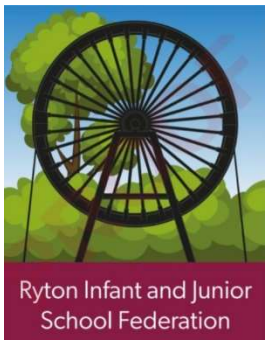
1. Staff, Governor and Visitor Acceptable Use Agreement
2. Acceptable Use Agreement: Pupils
3. Acceptable Use Agreement for Remote Learning and Online Communication

Last Reviewed: October 2020




The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at school with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse, such as online bullying, which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupil.




# 1. Teaching and learning

**Why the internet and digital communications are important**

1.1. The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

1.2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

1.4. Staff model safe and responsible behaviour in their use of technology during lessons

1.5. Teachers remind KS2 pupils about their responsibilities through an end-user Pupil Acceptable Use Agreement which every pupil will sign at the start of every academic year.

**Internet use will enhance learning**

1.6. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

1.7. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.

1.8. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

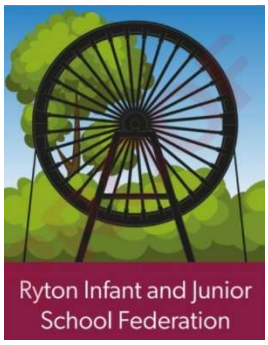
1.9. Pupils will be shown how to publish and present information to a wider audience.

**Pupils will be taught how to evaluate internet content**

1.10. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

1.11. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

1.12. Pupils will be taught how to report unpleasant internet content to a teacher or if appropriate the Headteacher. This can be done anonymously, or in person, and will be treated in confidence.




## 2. **Managing internet access**

### Information system security

2.1. School ICT systems security will be reviewed regularly.

2.2. Virus protection will be updated regularly.

2.3. Security strategies will be discussed with the IT provider.

### Email

2.4. Pupils do not have access to email on the school system

2.5. Incoming emails will be treated as suspicious and attachments not opened unless the author is known.

2.6. The school:

- Provides staff with an email account for their professional use (Microsoft 365) and makes clear personal email should be through a separate account.
- Does not publish personal email addresses of staff on the school website.
- Will contact the police if one of our staff receives an email that it considers is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up-to-date.
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous.

### Published content and the school website

2.7. Staff or pupil personal contact information will not be published. The contact details given online will be the school office.

2.8. The School Business Manager will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.

2.9. Uploading of information is restricted to our website authorisers.

2.10. The school website complies with the following statutory Department of Education guidelines for publications:

- What maintained schools must publish online

2.11. Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.

2.12. The point of contact on the website is the school address and telephone number. The school uses a general email contact address,

rytoncommunityinfantschool@gateshead.gov.uk
rytoncommunityjuniorschool@gateshead.gov.uk.

Home information or individual email identities will not be published.

2.13. Photographs published on the web do not have full names attached.

2.14. The school does not use pupils' names when saving images in the file names or in the tags when publishing to the school website.

2.15. The school expects teachers using school approved blogs or wikis to password protect them and run from the school website.

**Publishing pupils' images and work**

2.16. Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs.

2.17. Written permission or consent via Parentmail from parents will be obtained before photographs of pupils are published on the school website.

2.18. Pupil image file names will not refer to the pupil by name.

2.19. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

2.20. The school gains parental permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school.

2.21. The school does not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs.

2.22. Staff sign the school's Staff, Governor and Visitor Acceptable Use Agreement, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils Appendix 1

2.23. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

2.24. Pupils are taught about how images can be manipulated in their e-safety education programme and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

2.25. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

2.26. Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. The school teaches them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

**Social networking and personal publishing**

2.27. The school will control access to social networking sites and consider how to educate pupils in their safe use.

2.28. Newsgroups will be blocked unless a specific use is approved.

2.29. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

2.30. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

2.31. Pupils will be advised to use nicknames and avatars when using social networking sites.

2.32. Staff will be reminded of the risks of accepting parents and children as 'friends' on social networking sites, will be strongly advised not to do so, and given advice when needed on how to ensure their privacy settings only allow friends to access their pages

2.33. Staff will be advised to protect their profile information from the public by maximizing privacy settings. It is also good practice to choose an unidentifiable photo for profile and cover photos

2.34. Staff will be encouraged to 'untag' themselves from any inappropriate pictures that may appear on social networking sites.

2.35. Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school's preferred system for such communications.

2.36. School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or LA.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

**Managing filtering**

2.37. If staff or pupils come across unsuitable online materials, the site must be reported to the School Admin team who will liaise with our IT provider to block the site

2.38. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing videoconferencing and webcam use**

2.39. We will use Microsoft Teams for Video Conferencing as part of our Remote Learning Offering and where face to face meetings are not appropriate.

2.40. All staff using Microsoft Teams to communicate with pupils and parents will sign the Acceptable Use Policy for Remote Learning and Online Communication – Appendix 3

2.41. All participants will be made aware that Microsoft Teams can be used to record meetings. Recordings will only be stored for as long as necessary for other pupils to access the lesson. They will only be stored on Ryton Federation platform

2.42. Staff should use work provided laptops for video conferencing. Lessons or other meetings should not be recorded on personal equipment under any circumstance

2.43. Access to Ryton Federation Teams will be managed securely by

Pupils and Staff using strong passwords and not sharing passwords

Pupils and staff not logging in by using another member of staffs user name/ password

Pupils and staff logging off devices when not in use

2.44. Staff will record the length, time and date, attendance of any Teams sessions. This should be logged on the password protected Ryton Federation Sharepoint

2.45. Live 1 to 1 video conferencing sessions will only take place with the approval of the Designated Safeguarding lead and where possible a parent should be present

2.46. Access links to Teams sessions will not be made public or shared by participants.

2.47. Pupils are encouraged to attend sessions in a shared/ communal space or room with a door open and to be supervised by parents and carers or another appropriate adult

**Managing emerging technologies**

2.48. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

2.49. The SLT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.

.

**Protecting personal data**

2.50. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

**Personal devices and mobile phones**

2.51. The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Executive Headteacher. Such authorised use is to be monitored and recorded.

2.52. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.

2.53. Where parents or pupils need to contact each other during the school day, they should do so only through the school's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.

2.54. Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or on silent at all times.

2.55. Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

2.56. The Bluetooth, or similar function, of a mobile phone will be switched off at all times and not be used to send images or files to other mobile phones.

2.57. No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

2.58. If a member of staff breaches the school policy, disciplinary action may be taken.

2.59. Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities or parent's evenings where there are insufficient lines in school they should use their own device and withhold their own mobile number for confidentiality purposes.

2.60. Pupils will abide by the following rules when bringing a personal device to school:

- The school strongly advises that pupil mobile phones should not be brought into school; however, we accept that there may be circumstances in which a parent wishes their child to have a mobile phone for their own safety. Phones need to be stored in the school office until the end of the day.

- If a pupil needs to contact their parents, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in the safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

## 3. Policy decisions

### Authorising internet access

3.1. All staff will read and sign the Staff, Governor and Visitor Acceptable Use Agreement before using any school ICT resource – Appendix 1

3.2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

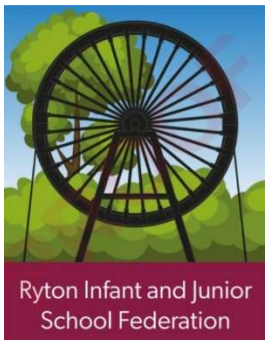
3.3. At EYFS and KS1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

3.4. Any person not directly employed by the school will be asked to sign the Staff, Governor and Visitor Acceptable Use Agreement before being allowed to access the internet from the school site.

### Assessing risks

3.5. The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of internet access.

3.6. The school should audit ICT use to establish if the E-safety Policy is adequate and that the implementation of the E-safety Policy is appropriate and effective.




**Handling e-safety complaints**

3.7. Complaints of internet misuse will be dealt with by a senior member of staff.

3.8. Any complaint about staff misuse must be referred to the Executive Headteacher.

3.9. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

3.10. Pupils and parents will be informed of the complaints procedure (see school's complaints policy)

3.11. Pupils and parents will be informed of the consequences for pupils misusing the internet.

3.12. Discussions will be held with the police youth crime reduction officer to establish procedures for handling potentially illegal issues.

**Community use of the internet**

3.13. The school will liaise with local organisations to establish a common approach to e-safety, if necessary.

## 4. Pupil online safety curriculum

**Teaching and learning**

4.1. This school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to the age of the children, including:

- To STOP and THINK before they CLICK.
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.

- To know how to narrow down or refine a search.
- To understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse, including online bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.

4.2. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.

4.3. The school will remind pupils about their responsibilities through a Pupil Acceptable Use Agreement which every KS2 pupil will sign – Appendix 2

4.4. All staff will model safe and responsible behaviour in their own use of technology during lessons.

**Online risks**

The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will support and enable children to use these technologies for entertainment and education but will also teach children (in PSHE) that some adults and young people will use such outlets to harm children.

**Cyber bullying and abuse**

4.5. Cyber bullying can be defined as "Any form of bullying which takes place online or through smartphones and tablets." - BullyingUK

4.6. Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/LA child protection procedures.

4.7. Through the PSHE curriculum, children are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.

4.8. Cyber bullying will be treated as seriously as any other form of bullying and will be managed through our anti-bullying and confiscation procedures. Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

4.9. There are clear procedures in place to support anyone in the school community affected by cyber bullying.

4.10. All incidents of cyber bullying reported to the school will be recorded.

**Sexual exploitation/sexting**

4.11. Sexting between pupils will be managed through our anti-bullying and confiscation procedures.

4.12. All staff are made aware of the indicators of sexual exploitation and all concerns are reported immediately to the DSL.

4.13. There are clear procedures in place to support anyone in the school community affected by sexting.

4.14. All incidents of sexting reported to the school will be recorded.

**Radicalisation or extremism**

4.15. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism leading to terrorism.

4.16. Extremism is defined by the Crown Prosecution Service as "The demonstration of unacceptable behaviour by using any means or medium to express views which:

- Encourage, justify or glorify terrorist violence in furtherance of beliefs.
- Seek to provoke others to terrorist acts.
- Encourage other serious criminal activity or seek to provoke others to serious criminal acts.

- Foster hatred which might lead to inter-community violence in the UK."

4.17. The school understands that here is no such thing as a "typical extremist": those who become involved in extremist actions come from a range of backgrounds and experiences, and most individuals, even those who hold radical views, do not become involved in violent extremist activity.

4.18. The school understands that pupils may become susceptible to radicalisation through a range of social, personal and environmental factors – it is known that violent extremists exploit vulnerabilities in individuals to drive a wedge between them and their families and communities. It is vital that school staff can recognise those vulnerabilities.

4.19. Staff will maintain and apply a good understanding of the relevant guidance to prevent pupils from becoming involved in terrorism.

4.20. The school will monitor its RE curriculum and assembly policy to ensure that they are used to promote community cohesion and tolerance of different faiths and beliefs.

4.21. Senior leaders will raise awareness within the school about the safeguarding processes relating to protecting pupils from radicalisation and involvement in terrorism.

## 5. Communications policy

Introducing the E-safety Policy to pupils

5.1. E-safety rules and guidance posers will be displayed and discussed with pupils regularly. An e-safety display will be kept up-to-date in one space

5.2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.

5.3. A programme of training in e-safety will be developed by the computing coordinator, PSHE coordinator and DSL.

5.4. Safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

**Staff and the e-safety policy**

5.5. All staff will be given the school E-safety Policy and have its importance explained.

5.6. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.

5.7. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

5.8. Staff will always use a child friendly safe search engine when accessing the web with pupils.

**Enlisting parents' support**

• Parents' attention will be drawn to the school E-safety Policy in the school brochure and on the school website and by offering E safety guidance sessions

• The school will maintain a list of e-safety resources for parents.

| Resource | Website |
|---|---|
| Child Exploitation and Online Protection Centre | www.ceop.gov.uk/ |
| Childnet | www.childnet-int.org/ |
| Digizen | www.digizen.org/ |
| Kidsmart | www.kidsmart.org.uk/ |
| Think U Know | www.thinkuknow.co.uk/ |
| Family Online Safety Institute | http://www.fosi.org |
| Internet Watch Foundation | www.iwf.org.uk |
| Internet Safety Zone | www.internetsafetyzone.com |
| Vodafone digital parenting | www.vodafone.com/content/digital-parenting.html |
| NSPCC - Share Aware | www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware |
| Parent Zone | www.theparentzone.co.uk/school |

## 6. Monitoring and Review

This Policy will be reviewed annually
Date of Next Review October 2021

# Appendix 1

## Staff, Governor and Visitor Acceptable Use Agreement

ICT and the related technologies, such as email, the internet and mobile devices, are an expected part of daily working life in school. This policy is to help ensure that all staff are aware of their professional responsibilities when using any form of ICT and to help keep staff, governors and visitors safe. All staff are expected to sign this agreement confirming their undertaking to adhere to its contents at all times. Any concerns or clarification should be discussed with the Executive Headteacher.

- I will only use the school's email, internet, learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my personal details, such as mobile phone number or personal email address, to pupils.
- I will only use the approved email system for any communications with pupils, parents and other school-related activities.
- I will ensure that personal data (such as data held on the administration system) is kept secure and is used appropriately. Personal data can only be taken out of the school or accessed remotely when authorised by the Executive Headteacher or Governing Body and with appropriate levels of security in place.
- I will not install any hardware or software on school equipment without the permission of the Executive Headteacher.
- I will report any accidental access to inappropriate materials immediately to my line manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with data protection policy and with written consent of the parent or staff member. Images will not be distributed outside the school network without the permission of the parent, member of staff or Executive Headteacher in line with data security policy.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to the Executive Headteacher.
- I will respect copyright and intellectual property rights.
    - I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. This includes ignoring invitations from pupils and parents to be part of their social networking site(s).
    - I will support and promote the school's E-safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.

**User signature**

I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

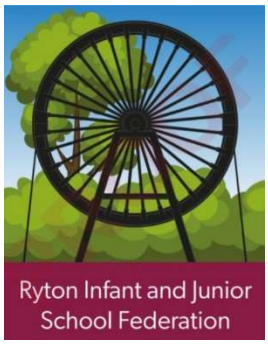
Signature _____

Date _____

Full name _____ (Printed)

Last Reviewed: October 2020

## Appendix 2




# Acceptable Use Agreement: Pupils

Class: _____

Year: _____

**Pupil Acceptable Use Agreement**

- I will only use ICT in school for school purposes.
- I will not tell other people my passwords for the school network or for other learning websites.
- I will only open/delete my own files.
- I will make sure that all ICT related contact with other children and adults is appropriate and polite.
- I will not deliberately look for, save or send anything that could offend others.
- If I accidentally find anything inappropriate on the internet I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number, home address or school.
- I will be responsible for my behaviour when using ICT in school or at home because I know that these rules are to keep me safe.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I know that my use of ICT can be checked and that my parent contacted if a member of school staff is concerned about my safety.
- If I bring a mobile phone or other personal ICT device into school I will hand it into the school office first thing each morning.

Signature pupil: _____

Date: _____

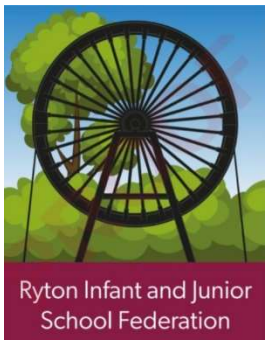
Ryton Infant and Junior School Federation

**Appendix 3**

# Ryton Federation Acceptable Use Policy (AUP)

# for Remote Learning and Online Communication

Last Reviewed: October 2020




**Leadership Oversight and Approval**

1. Remote learning will only take place using the Microsoft Teams platform and other online learning sites such as TTRockstars, Spelling Shed and Reading Plus, which have been assessed and approved by the executive head teacher, Mrs Deborah Ashcroft.
2. Staff will only use Ryton Federation managed accounts with learners and/or parents/carers (Ryton Federation Office 365 email accounts, Parentmail or Ryton Federation Teams account)
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with Mrs Deborah Ashcroft, Designated Safeguarding Lead (DSL).
    - Staff will use work provided laptops to provide remote learning.
3. Online contact with learners will not take place outside of the operating times as defined by SLT:
    - 9am- 3pm on days within the school term

   Teachers will provide one English and one Maths lesson daily plus a Foundation subject activity and the opportunity to share Foundation subject work online.

4. All remote lessons will be formally timetabled; the designated safeguarding lead/ deputy leads are able to drop in at any time.

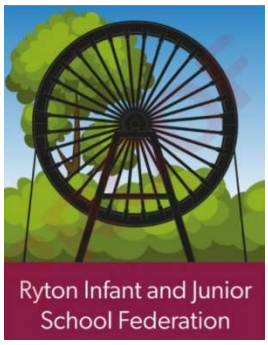
**Data Protection and Security**

5. Any personal data used by staff and captured by Microsoft Teams when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
6. All remote learning and any other online communication will take place in line with current Ryton Federation confidentiality expectations.
7. All participants will be made aware that Microsoft Teams can be used to record meetings. Recordings will only be stored for as long as necessary for other pupils to access the lesson. They will only be stored on the Ryton Federation Teams platform. Only pupils and staff within the class Team will be able to access the recordings.
8. Staff will not record lessons or meetings using personal equipment under any circumstance
9. Only members of the Ryton Federation community will be given access to Ryton Federation Teams platform.

10. Pupils do not have access to Outlook via their Teams login
11. Access to Ryton Federation teams will be managed securely by the following:
    - Pupils and staff using strong passwords and not sharing their passwords
    - Pupils and staff not logging on by using another member of the school community's username/ password
    - Pupils and staff logging off or locking devices when not in use

**Session Management**

12. Staff will record the length, time, date and attendance of any sessions held. This information will be stored on the password protected Ryton Federation Sharepoint platform, which can only be accessed by staff.
13. When live streaming with learners:
    - contact will be made via learners' class Teams site
    - Parents will be informed of the time of live streamed lessons via Teams or Parentmail
    - staff may mute/disable learners' videos and microphones when appropriate.
    - 2 members of staff will be present wherever possible (teaching assistants will be given school laptops to participate in lessons)
    - Live 1 to 1 sessions will only take place with approval from Mrs Deborah Ashcroft, Designated Safeguarding Lead. Where possible, parents should be in the room when such sessions take place.
14. A Teams invitation/ Parentmail message detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
        - Learners and/or parents/carers should not forward or share access links.
        - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
15. Alternative approaches and/or access will be provided to those who do not have access.
    - Paper based packs of worksheets
    - Recordings of lessons available for those who cannot attend at the time (on the class Teams site for a limited period of time)




**Behaviour Expectations**

16. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
17. All participants are expected to behave in line with existing Ryton Federation policies and expectations. This includes:
    - Appropriate language and content will be used by all attendees.
    - Staff will not take or record images for their own personal use.
18. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
19. When sharing videos and/or live streaming, participants are required to:
    - wear appropriate dress.
    - ensure backgrounds of videos are neutral (blurred if possible).
    - ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.
20. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

**Policy Breaches and Reporting Concerns**

21. Participants will be encouraged to report concerns during remote and/or live streamed sessions:
    - Informing a parent/ carer
    - Informing the class teacher
    - Informing Mrs Deborah Ashcroft, the designated safeguarding lead
    - If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to Mrs Deborah Ashcroft, the designated safeguarding lead
22. Inappropriate online behaviour will be responded to in line with existing policies such as Code of Conduct, Whistleblowing, and Behaviour Policies.
    - Sanctions for deliberate misuse may include restricting or removing the use of the Ryton Federation Teams site.
23. Any safeguarding concerns will be reported to Mrs Deborah Ashcroft, Designated Safeguarding Lead, in line with our child protection policy.

**I have read and understood the Ryton Federation Acceptable Use Policy (AUP) for remote learning.**

Staff Member/Parent Name: ……

Date……

Last Reviewed: October 2020